

REMARKS

Claims 1-29 were originally pending in the present application. Claim 22 has been amended, and claims 23-28 have been cancelled. New claims 30 and 31 have been added. Claims 1-22 and 29-31 are, accordingly, currently pending in the present application.

Section 112 Rejection

Claim 22 was rejected under 35 U.S.C. § 112 as being indefinite. Claim 22, a dependent apparatus claim, has been amended to correct its dependency upon claim 1, a method claim. Claim 22 now properly recites that it is dependent upon claim 21, and applicant now believes it to comply with Section 112.

Section 102(e) Rejection

The Examiner rejected claims 1-28 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,304,973 to Williams (herein referred to as the “Williams patent”). Applicants respectfully traverse.

Claims 1 and 11: With regard to independent claims 1 and 11, the Williams patent fails to disclose “authenticating an identifier for said packet” as recited in both claims. The section cited by the Examiner, Column 23, Lines 2-7 of the Williams patent, does not disclose this limitation. The Williams patent reads:

Discretionary Access Control is then performed by security device by verifying that the host has a receive association for the source IP address in the incoming packet’s IP header, step 152. If not, an audit is generated, step 162, and the processing flow is terminated, step 164.

Column 23, Lines 2-7. In other words, the “security device” in the Williams patent merely takes the source IP address in the packet—and ascertains whether the source address is on a list of authorized IP addresses before proceeding to process the packet. See FIG. 10 in the Williams patent.

This is consistent with and no different than the operation of many conventional firewalls. As pointed out in the background section of the present specification, a firewall that merely accepts the source address of a packet at face value is unsatisfactory because it is not capable of preventing address “spoofing.” See Specification at pages 2-3. An intruder can create a packet with a falsified source IP address, a “spoofed” source address, and thereby obtain illegitimate access to the protected host.

Merely accepting the source IP address as valid is not the same as “**authenticating**” it. As would be understood by one of ordinary skill in the relevant art, authentication of the source

address, or any other packet identifier, would require that the identifier be proven to be “authentic”. A packet could not merely assert that it came from some source address; it would have to present some form of credential that “proves” that it came from that source address. Such a credential, in accordance with one embodiment of the present invention, comes in the form of a cryptographic certificate.

In the Williams patent, there is no determination at all as to whether the source IP address is an “authentic” one or not. Instead, the source IP address is presumed correct and the security policy decision of whether or not to permit access control is based on the source IP address—regardless of the authenticity of the address specified in the packet.

Accordingly, applicant respectfully submits that independent claims 1 and 11 represent allowable subject matter. Claims 2-9 and 12-19 are dependent upon these claims, and, accordingly also are believed to represent allowable subject matter. Several of these dependent claims, as discussed below, include further limitations that highlight important distinctions between the present invention and the Williams patent:

Claims 2 and 12: Dependent claims 2 and 12 further recite the steps of “comparing said identifier to a list of identifiers” and “determining whether to send said packet ... in accordance with such a comparison” and at least one “policy rule”. Thus, as set forth in the claims, such a step of comparing the packet identifier to a list of authorized identifiers is a separate step from the step of “authenticating” the packet identifier. Thus, this further highlights that the mere comparison of the source IP address to a list of authorized IP addresses, as disclosed in the Williams patent, cannot be characterized as “authenticating” the packet identifier. The distinction between the two is made clear from the claim language itself.

Claims 3 and 13: Claims 3 and 13 recite the further limitation of “wherein said identifier is a common host identifier.” The Williams patent does not disclose such a usage of “common host identifiers” as that term is understood by one of skill in the relevant art.

Claims 4 and 14: Claims 4 and 14 recite the further limitation of “wherein said authenticating is performed in accordance with IPSEC standards.” The passages cited by the Examiner from the Williams patent do not discuss authentication or performing authentication “in accordance with IPSEC standards.” The passages read as follows:

FIG. 5 shows the preferred protocol headers for host-to-host messages and for control messages. All packets have an Ethernet or Token Ring header, as appropriate, with the standard Ipv4 (internet Protocol version 4) header and an IP Security (IPSec) header extension with an Common IP Security Option (CIPSO) label, as specified by RFCs

1825-1829. Different packet formats, as yet unspecified, will be used for the Type 1 model of the security device 18.

Column 11, Lines 60-67. Thus, the Williams patent merely indicates that it is preferable to utilize an IPSEC header extension to encrypt the contents of the packet.

Claims 5 and 15: Claims 5 and 15 recite the further limitations of (i) “retrieving a pointer to a security association from an authentication header from said packet”, (ii) “retrieving a key associated with said security association” and (iii) “determining whether said packet is authentic using said key.” The above steps are performed in order to authenticate a packet identifier.

The Examiner cites to Column 11, Lines 5-35 and Column 12, Lines 1-3 of the Williams patent as fully disclosing all of these limitations. Applicants respectfully disagree. As discussed in the Williams patent, a “key exchange protocol” is performed to generate unique keys known only to a pair of security devices. Column 11, Lines 5-9. “These keys are henceforth used to encrypt all communication between the attached hosts at the chosen security level” Column 11, Lines 9-11. The Williams patent then goes on to discuss the security advantages of assigning a unique set of keys to pairs of hosts.

Thus, the discussion of keys in the Williams patent is directed to using the keys to **encrypt** the contents of packets between pairs of hosts. On the other hand, the claim language in claims 5 and 15 specifically recites that the key is utilized to **authenticate** the packet—not to encrypt the packet. In fact, the present invention can be utilized where no communications are encrypted at all. It is only in dependent claims 8, 9, and 18, 19 where encryption and decryption are implicated in the present invention, and, notably, claims 8 and 18 require decryption of packets “prior to authenticating.”

Claims 6 and 16: Claims 6 and 16 recite the limitations of sending a first message to a third device “indicating said identifier is not authentic” when authentication of the packet identifier fails. The sections cited by the Examiner as disclosing these limitations do not discuss authentication or the sending of a message to a third device when an identifier is determined to be not authentic.

Thus, claims 1-20 are believed to contain allowable subject matter, and applicant respectfully requests allowance of these claims.

Claim 21-22: Independent claim 21 is directed to a “packet filter for a distributed firewall” which contains a memory segment storing a program for decrypting a “common host identifier” and for “authenticating said common host identifier”. As discussed more fully above, the Williams patent does not disclose “authenticating” a “common host identifier.”

Nor does it disclose a “first memory segment containing a list of common host identifiers” as recited in claim 21. The Examiner cites Column 25, Lines 37-46 as disclosing this limitation. The “profiles” referred to in this section are database records of persons permitted to access the secure system and are not the same as a “list of common host identifiers.”

Thus, claim 21 is believed to contain allowable subject matter. Claim 22 is dependent upon claim 21, and, accordingly, is also believed to contain allowable subject matter. Claims 23-28 have been cancelled.

Section 103(a) Rejection

The Examiner rejected claim 29 under 35 U.S.C. § 103(a) as being unpatentable over the Williams patent in view of U.S. Patent No. 5,606,668 to Shwed (herein referred to as the “Shwed patent”). Applicants respectfully traverse.

Claim 29 recites a “packet filter processor” coupled to an “encryption means for decrypting and authenticating a packet”. As discussed more fully above, the Williams patent does not disclose encryption means for “authenticating a packet”. Rather, where the Williams patent discusses authentication, it discusses it in the context of authentication of a “principal”, in other words authentication of a person as shown in FIG. 13 (see elements 512 and 522). See Column 25, Lines 15-46. The person must show certain credentials, namely a card or password, in order to obtain access to the system. The Williams patent does not disclose an encryption means that authenticates **packets**.

Nor does the Shwed patent apparently disclose this either. The Shwed patent appears to be directed to a conventional packet filter where security rules can be specified in what are perceived to be a more advantageous manner. See Background and Summary of the Invention.

Applicant respectfully submits that claim 29 represents allowable subject matter. New dependent claims 30 and 31 have been added that represent claim language similar to claims 5 and 7. These new claims, since they are dependent upon claim 29, are also believed to contain allowable subject matter.

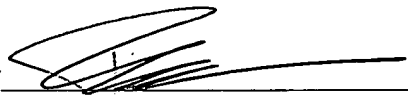
Conclusion

Applicants have addressed the rejections of the Examiner and, accordingly, a timely notice of allowance is earnestly solicited. The Examiner is invited to contact the undersigned at 908-532-1904 to discuss any matter concerning the application.

The Office is hereby authorized to charge any additional fees or credit any overpayments under 37 C. F. R. 1.16 and 1.17 to **AT&T Corp. Deposit Account No. 01-2745**.

Respectfully submitted,
Steven M. Bellovin

Date: May 30, 2003

By 
Benjamin S. Lee
Reg. No. 42,787

AT&T CORP.
P.O. Box 4110
Middletown, NJ 07748
Tel: 908-532-1904
Fax: 732-368-6932